(2)

POTENTIAL THREATS TO OFFSHORE PLATFORMS

Brian Michael Jenkins

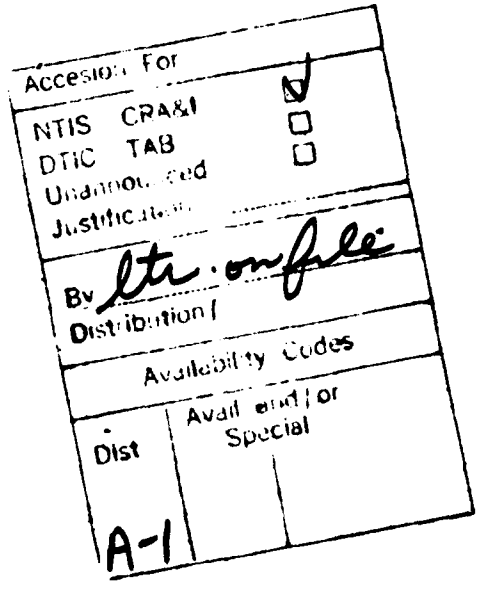
January 1988

P-7406

The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

PREFACE

This paper will appear in Volume 8 of *TVI Report* and in the *World Air and Seaport Defence and Security Handbook* for 1989.



POTENTIAL THREATS TO OFFSHORE PLATFORMS[1]

Brian Michael Jenkins

Increasingly spectacular acts of terrorism have led to growing concern that terrorists will move beyond the symbols of society and directly attack its technological and industrial vulnerabilities. Offshore platforms have been frequently mentioned among the potential targets terrorists might attack. This concern, however, has not resulted in extensive research like that devoted to possible threats to nuclear facilities, which have also been frequently mentioned as possible future targets of terrorists. For one thing, offshore drilling does not invoke the fear inherent in the word "nuclear," a fear that translates directly into heavy security for the nuclear industry. Neither does the construction of offshore platforms provoke anything like the kind of protest generated by the construction of nuclear facilities. In addition, offshore platforms are not easily accessible targets. Most important, the seizure or destruction of an offshore platform does not pose a direct danger to public safety. As a result, there are few published studies of platform security, apart from one completed more than ten years ago,[2] and a handful of articles. The unpublished literature is more extensive, but much of it is classified or proprietary.

There are several ways to analyze possible threats to offshore platforms. One approach would be to examine the past threats and incidents that have occurred at offshore platforms. A historical review of this type is free of speculation and establishes the criteria for minimum security measures. Relying exclusively on a historical

[1]The author wishes to acknowledge the helpful comments of Robert G. Moore, Fred Bornhofen, Frank Zapalac, Herb Force, and Ken Gillespie.

[2]The study was completed in 1976 by J. Christian Kessler, an analyst at the Center for Naval Analysis in Washington, DC. It is classified For Official Use Only and therefore is not in the public domain. See the Bibliography for additional references.

approach, however, does not necessarily provide a basis for anticipating possible future actions.

A second approach would be to examine the threats and incidents that are in any way analogous to possible actions against offshore platforms. For example, we could look at the history of actions directed against the oil and gas industry or of actions carried out in a maritime environment.

A third approach would be to extrapolate from what has occurred and develop a theoretical portrait of potential adversaries and the possible actions they might take against offshore platforms. This could help to identify the full range of potential threats and possible contingencies. It could also help establish the upper bounds for security measures. To what level of threat should security be provided? Beyond a certain point in the spectrum of threats, security becomes too costly or simply impractical.[3]

INCIDENTS AT OFFSHORE PLATFORMS

Although there have been few reported attacks on offshore platforms, the array of threats is quite diverse. Not unexpectedly, bomb threats have been the most common. In 1983, a bomb threat was made against a construction barge involved in the installation of the Chevron Oil platform *Edith* off the coast of California. The threat may have derived from a labor dispute between the local pile drivers' union and Chevron because of the use of foreign labor in the construction of the platform. A search produced no bombs.

Extortion was apparently the motive in a bomb threat made against offshore platforms belonging to Sun Oil in California. The extortionist

---

[3]The work done by The RAND Corporation on potential threats to nuclear programs followed this general approach, i.e., using actual history and analogous events to construct a theoretical profile of the threat. See Peter deLeon, et al., *Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs,* R-2225-SL, The RAND Corporation, February 1978; Gail Bass, et al., *Motivations and Possible Actions of Potential Criminal Adversaries of U.S. Nuclear Programs,* R-2554-SL, The RAND Corporation, February 1980; Gail Bass, et al., *The Appeal of Nuclear Crimes to the Spectrum of Potential Adversaries,* R-2803-SL, The RAND Corporation, February 1982.

reportedly had some knowledge of the facility. Two platforms were shut down while a thorough search was conducted. No money was paid and no bombs were found. Other platforms in California have been similarly threatened.

In 1981, British and Norwegian antiterrorist units were put on alert following a warning that Palestinian terrorists planned to blow up a North Sea oil installation. The anonymous caller, who was believed to be an Arab, on the basis of a voice analysis of a recording of the phone call, specifically warned that an offshore rig would be blown up. Operators of all oil rigs on the Norwegian and British continental shelf were instructed to search for bombs. There were no evacuations, and no bombs were found. In another incident, however, a fake bomb was found on one of the British North Sea platforms. Presumably, it had been planted by an employee.

British authorities take threats to North Sea platforms seriously. According to a report issued by British Petroleum Company in 1981, an explosion at a Scottish oil terminal near Inverness during a visit by the Queen may not have been due to equipment failure as originally reported; rather, it was apparently caused by a bomb for which the IRA originally claimed credit. Moluccan extremists are believed responsible for planting a limpet mine on a drilling rig in Rotterdam harbor.

Guerrillas in Angola in 1977 threatened to blow up the Cabinda offshore drilling complex operated by Gulf Oil Company. The company was warned to evacuate its 200 British and American employees. A spokesman for the guerrilla group mentioned the possible use of surface-to-surface missiles. The guerrillas wanted to shut down the operation because it was providing $2 million daily to the government they opposed. The guerrillas attacked harbor facilities and fuel reservoirs in 1980, and in 1985, the same guerrilla group claimed responsibility for shooting down a helicopter. All three people in the helicopter were killed. These attacks, however, were well south of the Cabinda complex.

Terrorists have not attempted to assault and take over an offshore platform--a scenario popular with novelists--although in 1981 a group of Greenpeace activists did attempt to board a Shell Oil rig 177 miles off the coast of Massachusetts. The group wanted to explain their

opposition to the drilling by holding a news conference on the rig. Shell officials denied the environmentalists access to the platform. Generally, one would place environmentalists low on the list of potential threats; however, some recent actions by environmentalists opposed to nuclear power and the whaling industry suggest that the threat of violence by environmentalist extremists is not to be dismissed.

The only takeover of an offshore platform occurred in Australia, where 330 workers occupied an offshore gas rig for three days during a labor dispute. The takeover was entirely peaceful and ended when the workers were threatened with heavy fines and warned that if they did not leave, they would never again work on any offshore platform. Production from the rig, which provides most of Western Australia's energy needs, was suspended during the occupation. Had the incident lasted, it would have had serious economic consequences.

Hostile employees are believed responsible for several minor incidents of sabotage at offshore platforms, one of which caused a one-hour shutdown.

The most serious attacks on offshore platforms have occurred in the Persian Gulf as a result of the war between Iran and Iraq. In 1987, U.S. warships shelled several platforms in retaliation for Iranian attacks on Gulf shipping. Wartime actions are a national security concern well beyond the responsibilities of any corporation, except as they illustrate particular vulnerabilities that may be exploited by nonstate actors.

Theft of equipment has also been a problem, particularly where there is a concentration of platforms. According to one report, thieves have chartered helicopters to reconnoiter offshore platforms, then returned at night to steal unattended equipment. Some of the equipment may even have to be sold to the original owners after it was refurbished and the serial numbers removed.

In addition to incidents at offshore platforms, attacks have also been made on other kinds of energy facilities in the maritime environment. Guerrillas operating at sea carried out attacks against port facilities (oil terminals and storage depots) in Cuba in the 1960s

and in Nicaragua in the 1980s. In both cases, the guerrillas received assistance from the U.S. government. In 1971, Palestinian extremists fired rockets from a speedboat at an oil tanker in the entrance to the Red Sea. The attack was intended to deter tankers from using the Israeli port of Eilat.

We have, then, the complete range of adversaries: guerrillas and terrorists (operating with or without state sponsorship), ordinary criminals, environmental extremists, and hostile employees. The actions to date include bomb threats, bombs, standoff attacks, mines, an attempt to board a platform, and a takeover (the boarding attempt and the takeover were both peaceful), and theft of equipment.

The meagre history, even allowing for unreported incidents, shows that attacks on offshore platforms are infrequent events. This perception was confirmed by private discussions with government and company officials, each of whom was able to recall only a few incidents, often the same ones recalled by the others.

ACTIONS AGAINST ENERGY FACILITIES: THE RAND CHRONOLOGY

A chronology of attacks on energy facilities compiled by The RAND Corporation allows us to take a broader look at the threats faced by the oil and gas industry. Although the chronology contains more than 200 incidents at oil and gas facilities since 1968, it cannot be considered complete. Sabotage is often disguised to appear accidental; bomb threats, a common problem in all industry, and extortion are generally underreported. It is doubtful that more than a fraction of the bombings are publicly mentioned.

Nonetheless, the chronology does show that a wide range of criminal activity has been directed against oil and gas facilities. Hostile employees have carried out acts of sabotage and, as noted above, on one occasion seized control of an offshore platform. Terrorists and guerrillas have bombed pipelines, pumping stations, storage depots, terminals, and refineries, as well as oil company offices; they have fired with mortars and rockets at tankers and tank farms; they have threatened to shoot down helicopters; they have assassinated and kidnapped oil company officials; they have mined waterways. Criminal

extortionists have planted bombs, made threats, shut down refineries; thieves have stolen both equipment and products.

For the most part, these adversaries have concentrated their attacks on targets that were easy to hit. Bombings of oil pipelines by guerrilla and terrorist groups comprise nearly half of all of the recorded incidents. Bombs planted at storage facilities are the second most common type of attack, accounting for approximately 13 percent of all incidents, followed by bombs placed at corporate headquarters and buildings that house oil company offices--a purely symbolic form of attack. Overall, bombings account for 75 percent of the total incidents.

Less than 4 percent of the attacks have involved bombs planted at large centralized facilities, such as refineries and terminals. In general, few attacks of any type--bombings, armed assaults, or mortar and rocket attacks--have been directed against central facilities. One may presume, however, that major facilities with large workforces are the principal theater of industrial sabotage, much of which is unreported.

Saboteurs in the workforce seldom do things that are calculated to harm people. In contrast, terrorists may see people, both executives and workers, as "soft targets." The RAND chronology includes eight kidnappings of oil company executives and seven shootings or assassinations. Most of the kidnappings were perpetrated for the purpose of collecting ransom; the victim's type of business has little relevance to the kidnappers. However, terrorists have also attacked people as a means of shutting down facilities they oppose on environmental or political grounds or because they want protection money on a regular basis. The latter seems to be the case where oil exploration and production overlap with guerrilla warfare. Another tactic seen in the Third World is overt armed assaults on drilling rigs. Guerrillas in Guatemala and Colombia have attacked crews at drilling sites; in some cases, they have temporarily seized control of the facilities. This type of attack is not common and is likely to be a potential threat only in remote areas where guerrilla forces are active.

Guerrilla groups have on numerous occasions fired at helicopters, and at least one of these attacks involved a helicopter that was servicing oil rigs. As hand-held precision-guided surface-to-air missiles become more widely available, we can anticipate more attacks of this type.

When denied direct access to their targets, terrorists typically have resorted to standoff attacks. The chronology lists seven standoff attacks, about 3 percent of the total incidents. As mentioned previously, one of these attacks involved a loaded oil tanker. Standoff attacks pose a threat to both personnel and equipment on platforms, and perhaps an even greater threat to floating storage tanks or tankers loading at a facility.

There have also been several recent incidents in which guerrilla and terrorist groups have affixed mines to the hulls of ships or planted floating mines at sea. Nineteen tankers were damaged by mines at the mouth of the Red Sea in 1984. Although the Islamic Jihad claimed credit for this operation, Libya was believed to be responsible for planting the mines. Antigovernment rebels in Nicaragua planted mines at the entrance to the Nicaraguan port of Corinto, an operation that was strongly criticized in the United States.

Disgruntled or hostile employees have the technical knowledge and access to carry out the most effective acts of sabotage. However, there have been few publicized reports of sabotage on offshore platforms.

OTHER STUDIES OF SABOTAGE

A 1980 study by Robert Mullen examined several hundred incidents of sabotage directed against energy facilities; that study reached some of the same conclusions noted above and added several observations.[4] Mullen showed that saboteurs have generally chosen operations that require few resources and only modest technical skills, entail minimum risk, and have good chances of success. For the most part, the

[4]See Robert K. Mullen, "Attributes of Energy Asset Saboteurs: An Historical Perspective," paper presented to the First International Congress on Physical Protection in Petroleum Installations, undated.

saboteurs have carried out their attacks covertly against simple, unprotected targets such as pipelines, powerlines, and remote substations.

Of 408 incidents reviewed in the study (204 in the United States and 204 in other countries), 248, or 66 percent, were aimed at pipelines, powerlines, or substations--"distributed targets" that are impossible to defend. Of the 139 attacks on oil and gas facilities, 81, or 60 percent, were directed against pipelines; 30, or 22 percent, were directed against oil and gas storage facilities; and only 24, or 17 percent, were directed against more complex centralized facilities such as refineries or oil wells.

Political protest was the most common motive of the attackers in the study, accounting for 59 percent of the recorded incidents. Labor action was the next most common motive, accounting for 28 percent of the incidents, followed by ordinary criminal motives, which accounted for 6 percent. However, one must be wary of a reporting bias here. Actions taken for the purpose of political protest are calculated to gain public attention and are carried out in ways that make them obvious. Sabotage carried out by hostile employees is often disguised to look like an accident. Acts of sabotage can be executed by employees who have the access and the technical knowledge to use methods that are not obvious, such as leaving valves open. Such acts may be recognized as sabotage only by a company's managers. Therefore, open sources of information would be expected to include more incidents resulting from protest than from labor strife.

In 99 percent of the cases examined in the Mullen study, the saboteurs operated with limited physical resources. The technical skills they demonstrated were assessed to be modest, rather than sophisticated, in 82 percent of the incidents. Explosive devices that failed to detonate or that were incorrectly placed were taken as evidence of poor technical skills. Again, however, there is a potential reporting bias, as most of the reported cases are actions by political extremists whose technical knowledge is likely to be limited. Actions taken by hostile employees may be both effective and invisible. Nor should the fact that saboteurs generally operate with modest resources

necessarily mean that their actions are ineffective--effective sabotage need not always be sophisticated.

Consistent with the modest physical resources and low technical skills displayed in the attacks, the planning and management skills demonstrated were judged to be modest in 92 percent of the cases.

Security measures are apparently effective in deterring some of the adversaries. For the purpose of analysis, Mullen's study identified four levels of security:

1. Unrestricted access.
2. Simple restrictions (e.g., a passive physical barrier).
3. Restrictions and manned security (e.g., fences and guards).
4. Restrictions and manned security, plus compartmented access (e.g., interior coded access).

Fifty-two percent of the incidents were carried out against targets that offered unrestricted access; 26 percent were carried out against targets protected only by a fence or some other passive barrier; 18 percent were carried out at facilities protected by both physical barriers and guards; and only 4 percent were carried out at facilities protected by more extensive measures. If the data had not included incidents resulting from labor strife, in which the attackers probably were "insiders" with legitimate access to the targets, the correlation between the frequency of attack and the level of security would have been even stronger.

Not surprisingly, the study showed that sabotage carried out by insiders was more effective (physical damage was accomplished in 96 percent of the cases) than sabotage carried out by outsiders (who accomplished physical damage in 73 percent of the cases).

A separate study of peacetime sabotage provides additional information on the attributes of saboteurs.[5] In that study, hostile employees accounted for one-third of the 37 incidents reported while political extremists accounted for 27 percent. The saboteurs included

---

[5] deLeon, op. cit.

ordinary criminals, individuals acting for various personal reasons, and in at least one case, foreign agents. The motives match: Labor strife was the principal motive attributed to the saboteurs, followed by political protest and economic gain.

Most of the reported incidents occurred in remote areas against easily accessible, unguarded targets. Confirming the Mullen study, this study notes that none of the attacks occurred at facilities with sophisticated alarm systems. One must again be cautious of a reporting bias: To avoid embarrassment, companies may hesitate to report incidents at facilities that are supposed to be well-protected.

One-third of the incidents in which the number of perpetrators was known were carried out by one individual. Many incidents, particularly those involving labor strife, involved more than one individual, but not because more were necessary to accomplish the task. In most cases, one person could have done it alone.

The saboteurs were known to have possessed weapons in only two of the 37 cases. In most cases, weapons were irrelevant. In only one case did the saboteurs have to neutralize a guard. In half the cases, they employed explosives to carry out the sabotage; in the other half, they used simple hand tools.

The objective of the saboteurs was to disable the facility they attacked or to disrupt its operations. With one exception, where the motive was personal revenge against one worker, the saboteurs showed no desire to risk their own lives or the lives of others.

Since many of the saboteurs were employees, the study assumed they possessed the necessary knowledge to carry out their attacks. In the remaining cases where the saboteurs were not employees, the knowledge required for the type of attack carried out was usually publicly available. Highly specialized knowledge was required in only a few cases. Little planning was evident in any of the attacks. For the most part, the saboteurs merely attacked targets of opportunity. With one possible exception, there was no evidence of any operational training.

Despite the low levels of planning and training, the saboteurs were successful in all of the cases, in that they caused some damage. In only one out of five cases were the saboteurs apprehended.

SUMMARY OF PAST ACTIONS AGAINST OFFSHORE PLATFORMS

Before constructing a theoretical portrait of potential adversaries, we summarize below the findings from our examination of incidents that have occurred at offshore platforms and our review of other studies of sabotage.

Security planners confront a broad array of adversaries: guerrillas and terrorists, disgruntled or hostile employees, ordinary thieves and extortionists, environmentalist extremists, individuals with idiosyncratic motives, and potentially, agents of a hostile state. Although two of our data sources indicate political protest (i.e., actions by guerrillas or terrorists) as the most frequent motive for sabotage, actions carried out by disgruntled or hostile employees are probably the most common. They are simply harder to identify due to the difficulty of determining cause in sabotage carried out by employees and the likelihood of a reporting bias. Numbers of attackers were not a critical constraint. One person could singlehandedly carry out most of the sabotage seen. When necessary, larger groups have been mobilized.

For the most part, the adversaries struck targets of opportunity in remote areas. Accessibility and avoiding confrontation with guards seem to be primary considerations. Far fewer attacks were carried out against centralized facilities that were protected by security systems. Offshore platforms are not easily accessible and are protected by natural barriers. Attacks have seldom been made against offshore platforms or other targets at sea, and the few reported incidents were generally indirect, i.e., bomb threats and standoff attacks.

Attacks on major centralized facilities have been made by saboteurs from long-established guerrilla or terrorist groups who had considerable experience and were sometimes assisted by a government.

Weapons were employed by guerrilla groups in the Third World but most saboteurs preferred to carry out their sabotage covertly, avoiding confrontation. They employed explosives or simple hand tools to accomplish their task.

Using knowledge they already had as employees or that was easily gained through simple reconnaissance, they exhibited little planning, little training, and low technical skills. Despite this, they were often successful--generally, because they hit easy targets. Even minimal levels of security deterred them.

THE SPECTRUM OF POSSIBLE ACTIONS

The incidents that have occurred at offshore platforms plus those directed against energy targets in general, and those in the maritime environment in particular, provide security planners with an indication of the spectrum of adversaries and actions they confront. These are summarized in the following figure, which identifies only the three most likely categories of saboteurs: hostile employees, terrorists, and ordinary criminals.

Agents of hostile foreign governments are not included, although in certain circumstances they represent the most serious--albeit a more remote--threat. Motives might include retaliation for attacks or participation in attacks on energy facilities; for example, if the United States, in response to state-sponsored terrorism, decided to bomb energy facilities in the country it accused of sponsoring the terrorists, that country might support operations against American energy facilities. One country may want to punish another for a specific policy, or it may want to prevent a country from gaining greater energy independence.

Bomb Threats and Bombings. Bomb threats are a common problem at virtually all industrial and commercial facilities. Threats are made to harass companies, to disrupt operations, to force evacuations that will give employees time off. Actual bombings, as we have seen, are the most common form of attack on energy facilities. Given the lack of public access to offshore platforms, employees who may be persuaded or coerced into acting on behalf of terrorists or a hostile government are the most likely culprits. Historically, however, attacks by employees have rarely occurred. More sophisticated adversaries with a capability for scuba operations conceivably could affix explosive charges to the

THE SPECTRUM OF POTENTIAL ADVERSARIES TO OFFSHORE PLATFORMS AND LIKELY ACTIONS

	Hostile Employees	Criminals	Political Extremists
Bomb threats	XXX	XXX	X
Bombs		XX	XX
Mines			XX
Peaceful attempts to board & armed assaults			XXX[1]
Standoff attacks			XXX[2]
Remotely piloted vessels or aircraft			XX
Manned vessels or aircraft			X
Offsite attacks on personnel			XX
Occupations & seizures with hostages	XXX		XX
Traditional sabotage	XXX		
Theft of equipment	X	XXX	

XXX = An adversary in this category has already carried out an action of this type at an offshore platform.

XX = An adversary in this category has already carried out an action of this type against an oil or gas facility or in a maritime environment.

X = An adversary in this category has already carried out an action of this type against another category of target.

---

[1]Environmentalists did attempt to board an offshore platform.

[2]Guerrillas threatened to use surface missiles against offshore platforms.

underwater portion of a platform. French agents did this to sink the *Greenpeace* in New Zealand, and a similar technique may have been used by environmentalist extremists in their attacks on whaling vessels in Iceland. A few guerrilla or terrorist organizations reportedly have received training in underwater demolition. Denied access to the platform itself, adversaries might try to place bombs on floating storage tanks, underwater pipelines, or terminal facilities on shore, or aboard vessels servicing offshore platforms.

Mines. As we have seen, floating mines have been used in both the Red Sea and off the coast of Nicaragua. Limpet mines attached to the hulls of ships have been used by right-wing Cuban fanatics and terrorist groups in Lebanon.

Sabotage. We can distinguish two levels of sabotage: Low-level sabotage comprising vandalism or other actions calculated to temporarily disrupt or disable a facility or simply to impose a financial cost on a corporation, and high-level sabotage comprising actions intended to destroy a facility, possibly endangering human life. Low-level sabotage is often the work of disgruntled employees, particularly during periods of labor strife. It rarely involves the use of explosives. High-level sabotage lies in the domain of terrorism or surrogate warfare by one nation against another. In the case of an offshore platform, it might be carried out surreptitiously by planting explosives underwater, or it might be preceded by an overt assault to temporarily seize control of a facility.

Peaceful Attempts to Board and Armed Assaults. Peaceful attempts to board a platform may be made by environmentalists or others protesting the construction or operation of the platform. Except in remote areas of the Third World, where guerrilla armies challenge government forces, overt armed assault has not been a common mode of attack on energy facilities. However, terrorists have carried out armed assaults on nuclear facilities in Argentina and Spain.

Standoff Attacks. Offshore platforms differ from other energy facilities that have been attacked by guerrillas and terrorists in one important respect: By their very nature, offshore platforms do not allow easy access. Direct access can be obtained only by subterfuge--

for example, the use of disguise--or by force; and even in the case of an armed assault, direct access can be easily channelized and blocked or delayed by the proper placement of barriers. When denied direct access to a preferred target, guerrillas and terrorists have typically resorted to standoff attacks, i.e., direct and indirect fire from weapons employed at some distance from the target. We may distinguish two levels of standoff attack: Low-level standoff attack includes the use of weapons from ordinary rifles up to the hand-held antitank weapons--rocket launchers, rocket-propelled grenades, etc.--commonly used by terrorists. The range of such weapons is usually less than 1,000 meters, and their explosive charges weigh no more than a couple of pounds.

High-level standoff attack includes larger crew-served weapons--mortars, larger rockets, recoilless rifles, and some of the newer antitank weapons that can be fired by one man. Such weapons have ranges of up to several kilometers and can deliver heavier explosive charges. The IRA's homemade mortars have delivered explosive charges weighing more than 40 pounds. Rockets could be fired from small boats; firing larger mortars would require that the hull of the launching vessel be reinforced to withstand the impact of the recoil.[6]

In 1978, Palestinian extremists sailed a ship into the Israeli port of Eilat. The vessel carried 120mm rockets, which were to be fired at oil storage tanks in the harbor. Its hold was filled with explosives which were to detonate as the ship went aground on the usually crowded beach. The operation was foiled when Israeli naval units challenged the vessel before it reached Eilat. This episode probably represents the highest level of resources and skill that any group outside of a national government can organize.

Standoff attacks may be directed against a platform itself, or against storage tanks or loading tankers moored nearby. This category also includes attacks on helicopters servicing a platform in which the attackers used conventional antiaircraft weapons or more sophisticated

[6]For a review of standoff weapons available to terrorists, see Thomas C. Tompkins, *Military Countermeasures to Terrorism in the 1980s*, N-2178-RC, The RAND Corporation, August 1984.

precision-guided munitions of the type that have been used by guerrillas in Zimbabwe, Afghanistan, Nicaragua, and Sudan.

Takeover of an Offshore Platform. Terrorists have hijacked airliners, trains, and ships at sea, and they have seized embassies. Why not offshore platforms? Several novels and at least one movie, *ffolkes,* offer scenarios in which terrorists take over an offshore platform, hold its crew hostage, and threaten its destruction if their demands are not met.[7] From the terrorists' point of view, offshore platforms would seem to offer several attractive features: An offshore platform would provide a dramatic venue for the terrorist operation, guaranteed to give the terrorists widespread publicity. Manned platforms have crews that could be held hostage. Just like an airplane fuselage, a platform seized by terrorists could be easily isolated and barricaded against attack. Communications facilities would be available for broadcasting propaganda and conducting negotiations. Platforms have their own power and contain food and other supplies that would permit the terrorists to withstand a lengthy siege. And in addition to threatening lives, the destruction of a major platform means millions of dollars in losses and economic disruption of potentially strategic proportions.

Continuing to look at the issue from the terrorists' point of view, however, offshore platforms also have a number of unattractive features: First are their natural defenses; they are surrounded by water--in some cases, considerable expanses of water. Terrorists have almost always entered or boarded their hijacking targets posing as ordinary civilians, but there is no routine public access to an offshore platform. To gain access, the terrorists would have to disguise themselves, for example, as company officials, as security forces, or as the crew of a disabled vessel; or they would have to openly assault the facility, which is something terrorists generally have not done.

---

[7]See, for example, W. A. Harrison, *The Oil Heist,* London: Corgi, 1978; and Alistair Maclean, *Seawitch,* New York: Fawcett Crest Books, 1977.

Offshore platforms are large, complex facilities. Taking one over would be difficult and would probably require a larger group of terrorists than is normally deployed. The isolated nature of an offshore platform would also make it difficult for the news media to cover the incident visually. This was demonstrated in the case of the *Achille Lauro*. The news media could provide distant views of the ship, but they could not obtain close-up views of hostages with guns held to their heads or conduct interviews with hostages, images that provide human drama and increase the terrorists' leverage over a government. And finally, an offshore platform offers no ready means of escape. It cannot be flown to a "friendly" country in which the terrorists will be permitted to escape. Escape from an offshore platform must be part of any other demands the terrorists negotiate. Terrorists face the same dilemma when they seize embassies or other buildings that can be surrounded by security forces. But "barricade-and-hostage" situations of this type declined in the 1980s as governments demonstrated greater resistance to meeting the demands of terrorists holding hostages and became more willing to use force to end such situations. As the risk of being killed or captured increased, terrorists gradually have abandoned the tactic. Although a terrorist "hijacking" of an offshore platform remains a theoretical possibility, the only takeover we have seen was carried out by angry employees.

Use of Remotely Piloted, Explosives-Filled Vessels or Aircraft. Basque separatists in Spain have employed small radio-controlled boats carrying a sufficient explosive charge to blow a hole in the side of a naval vessel. A fairly large charge would be necessary to cause major structural damage to an offshore platform, but this mode of attack might be employed against a floating storage tanker or other vessel near a platform. Remotely piloted aircraft are increasingly used by the military for reconnaissance. The basic technology is not complex. Conceivably, a large model aircraft or a small drone could be used by terrorists, particularly those with state sponsorship, to deliver an explosive charge to an offshore platform.

Use of Manned, Explosives-Filled Vessels or Aircraft. The suicide bombers of the Middle East raise the possibility of similar attacks on offshore platforms, using boats or airplanes. In fact, small, fast boats carrying large quantities of explosives and piloted by volunteers who aimed their craft, locked the wheel, and jumped overboard at the last minute, or in some cases remained with their craft until the end, were used with devastating effect against naval forces in the Mediterranean during World War II.[8] In the 1980s, explosives-laden trucks driven by suicide drivers have obliged security planners to contemplate suicide attacks on the ground or from the air. However, suicide bombers have not appeared outside of the Middle East, making this a regional rather than a global threat at present.

Offshore Attacks on Personnel. Terrorists may try to disrupt operations or indirectly disable a facility by directing attacks against key personnel when they are offsite. This strategy was used with great effect by the Basque separatist group ETA, which threatened to kill executives of a certain utility company if it did not halt construction on a nuclear facility which ETA opposed. Death threats were sent to all of the key officials. The kidnapping of one and the assassination of another underlined the threat. Work on the facility has been halted for several years.

Theft. Pilferage of equipment, often by employees, is a common problem in all industries. Professional thieves have carried out larger-scale thefts of major equipment from unmanned platforms.

THE STATE OF SECURITY

Although the approach discussed here gives an idea of the range of threats to offshore platforms, it does not allow an assessment of probability, except to note, as mentioned earlier, that such attacks appear to have been infrequent. Security measures reflect several considerations: (1) likelihood of attack--proximity to guerrilla or

[8]Richard O'Neill, *Suicide Squads*, New York: Ballantine Books, 1981. The Italian Navy developed and effectively employed explosive motorboats before and during World War II.

terrorist activity; (2) accessibility--distance from the shore, stormy seas, etc.; (3) type and value of the target--unmanned platform, production platform mobile drill rig, processing unit, floating storage unit; (4) strategic or economic importance; (5) environmental consequences; and (6) the utility of security measures.

The most advanced security measures and response planning have been implemented by the British government, specifically the Royal Navy, to protect offshore platforms in the North Sea. There are few of these platforms, and they are vital to the British economy. Continued terrorist activity by the IRA adds an element of real threat, although some observers say the North Sea security issue has also been exploited to justify budget increases.

The Indian government also has become concerned about the security of its platforms in the offshore fields near Bombay known as the Bombay High. The Indians perceive the Pakistanis as the principal threat and are worried about sabotage to either the platforms or the pipelines, which run for about 90 miles in shallow water. Without assessing Pakistan's intentions, we note that the Pakistanis do have the capability for seaborne sabotage. They possess a number of small Italian-built submarines that can each carry up to 12 frogmen.

Private oil companies generally have decided not to protect offshore platforms with high levels of security for a variety of reasons: (1) only a handful of low-level incidents--mainly bomb threats--have occurred and companies do not perceive a serious threat at present; (2) in some cases, for example, in the North Sea, the platforms are protected by formidable natural defenses; (3) down-hole shutoff devices prevent blowouts and sustained fires; (4) security systems such as radar, closed-circuit television, sonar, and sensors are costly to install and maintain, especially in a marine environment, and they require full-time personnel to monitor or operate, which means money; (5) available security systems are perceived to be of doubtful utility; (6) some measures--e.g., background checks on employees, exclusion areas around platforms--are prohibited or sharply constrained by law; and (7) where companies have many platforms, the temporary loss of one would not cause economic catastrophe to the company or strategic damage to any country.

Attitude may also be a factor. The comment, "Let Lloyd's [of London] pay for the first two [incidents] and then we will worry about it," reflects the view that rare events are best handled with insurance. Several serious incidents must occur before premiums go up and serious security measures become necessary.

The line of reasoning changes when (1) the perceived threat is greater; (2) adversaries may have easier access to the platform; and (3) the facility is critical.

To discourage unauthorized craft from approaching platforms, some companies maintain marine patrols; in some cases, local fishing vessels contract for the work. The primary function of these vessels is to rescue workers who have fallen from platforms, but they also contribute to security by monitoring and, where legal, challenging unidentified craft in the area. For safety reasons, some companies have established exclusion areas around their platforms which vessels are prohibited from entering, but this is sharply limited where platforms are close to navigation routes. A few companies operate radar on their platforms.

Many platforms have physical barriers--locked doors between the mooring area or helipad and the deck of the platform--to prevent easy access from the sea or air. Cranes may be swung across helipads to prevent unauthorized landings.

Companies generally make no provisions for resisting possible attack. In case of imminent attack, they plan to rely on what might be called a "passive defense," shutting down the platform (which can be done instantly) and evacuating all personnel, leaving the attackers with possession of a pile of iron and the authorities with the task of getting it back. In a few cases, however, where facilities are vital and threat levels are high, armed guards and response forces may be employed.

A few platforms have closed-circuit television and lights to monitor the landing dock and access routes. Underwater cameras are rarely used, and only in the few cases where the threat is considered serious is sonar equipment ever employed.

With rare exceptions, platform security measures do not include armed guards. Companies place primary reliance on the capability of the local police and military authorities to respond to any emergency at the platform. In at least one country, a foreign oil company contributes to the operational expenses of nearby military units to secure protection for its offshore facilities.

Judging by current security measures at existing platforms, the companies' biggest concern is the threat posed by employees with legitimate access to platforms. Vetting of employees is done where and to the extent that it is legal and permitted by labor contracts. Almost every company rigorously searches crews and cargo before transferring them to the platform. The principal concern is to prevent narcotics, liquor, and other contraband from getting to the platform. Here again, the motive is not fear of sabotage, but rather employee safety; however, such measures contribute to security as well.

To deal with bomb threats, the most common type of incident, most companies have developed search procedures in which all employees participate and have coordinated these with local law enforcement authorities.

Although offshore platforms seem vulnerable targets, theoretically attractive to a diverse group of potential adversaries, the actual history of criminal activity involving platforms does not support an assessment that the threat is high. Current security measures reflect this assessment. There are obvious exceptions where higher levels of security seem appropriate and have been imposed.

The situation may change as offshore activity expands, as the technological environment changes (as more helicopters and submersible craft are deployed), and as the conflict in the Persian Gulf provides examples and inspiration for future action.

SELECTED BIBLIOGRAPHY

Charm, Robert, "Terrorists See Offshore as Tempting Target," *OFFSHORE,* Vol. 43, p. 62(3), January 1983.

Chubin, Shahram, "The Iran-Iraq War and Persian Gulf Security," *International Defence Review 17,* 1984, No. 6, pp. 705-712.

"Iran Plugs Offshore Wells Exposed to Iraqi Missiles," (International News), *Wall Street Journal,* December 14, 1983, Section 2, p. 34(W); p. 35(E).

Jacobs, Michael J. and Thomas A. Watts-Fitzgerald, "Protection of Offshore Assets of the United States from Terrorist Activity," *National Resources Law,* Vol. 16, Winter 1984, pp. 569-595.

Jenkins, Brian Michael, et al., *A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets,* The RAND Corporation, P-6906, September 1983.

Keeney, Ralph L., et al., "Assessing the Risk of an LNG Terminal," Woodward-Clyde Consultants, San Francisco, CA., *Technology Review,* October 1978, Vol. 81, No. 1. p. 64.

Kessler, J. C., *Legal Issues in Protecting Offshore Structures,* Center for Naval Analyses, 1401 Wilson Boulevard, Arlington, VA 22209; June 1976, Prof. Paper, 42 pp. Available from National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161 (Report No. CNA-147; AD-AO28389/5ST)

Loftas, Tony, "The Threat to Europe's Oil Fields," *New Scientist,* Vol. 63, No. 912, August 29, 1974, pp. 513(3).

Macbain, M., "Will Terrorism Go to Sea?" *Security Management,* Vol. 24, No. 8, August 1980, pp. 76-77, 79-80, 82, 86-89, 91-94. Reprinted from *Sea Power,* January 1980.

MacNair, D. G., "Nature of the Beast--A Soliloquy on Maritime Fraud, Piracy and Terrorism," *Journal of Security Administration,* Vol. 5, No. 1, June 1982, pp. 41-47.

Maechling, Eugenie, "Security Risks to Energy Production and Trade: The Problems of the Middle East," *Energy Policy(UK),* Vol. 10, No. 2, June 1982, pp. 120-130.

Marriott, John, "The Defence of North Sea Oil and Gas," *NATO's Fifteen Nations,* Vol. 19, Oct-Nov 1974, pp. 72-79+.

Matt, A. R., "Maritime Terrorism--An Unacceptable Risk," Gulf Publishing Company, *Ocean Industry*, Vol. 16, No. 3, March 1981, pp. 93-98. (Available from University Microfilms International, 300 North Zeeb Road, Ann Arbor, MI 48106.)

Meadows, Ian, "Oil Field Security Becomes More Vital to Persian Gulf: Producers Plan Improvements," *Oil Daily*, January 28, 1982, pp. 1(2).

Nyhart, J. D. and J. C. Kessler, "Ocean Vessels and Offshore Structures," (in *Legal Aspects of International Terrorism*, 1978, by Alona E. Evans and John F. Murphy; Heath Lexington Books, American Society of International Law, Washington, DC 20008, 1978, 34 pp.

"Oil Industry Sleuths--Crime Prevention from Oil Rig to Pump," Security World Publishing Company, Inc., Los Angeles, CA 90034, *SECURITY WORLD*, Vol. 16, No. 11, November 1979, pp. 16-19.

"Saudis Intercede with Iraq to Halt Hits on Iran Offshore Wells," *Platt's Oilgram*, Vol. 61, April 4, 1983, pp. 2(1).

"United Arab Emirates to Build Big Naval Base to Protect Oil," *The New York Times*, Vol. 135, December 2, 1985, p. 6(N); p. A4(L).

Vaiana, P. J., *Electronics in Port Security--Marine Oil Terminals*, Radio Technical Commission for Marine Services; Federal Communications Commission; Washington, DC 20554. Continental Oil Company, 8 pp, 1978. (Available from Radio Technical Commission for Marine Services Federal Communications Commission, Washington, DC 20554.)

Wall, Patrick, "Defence of North Sea Energy Sources: The Military Aspects of the Problem," *NATO's Fifteen Nations*, Vol. 21, April-May 1976, pp. 78-83.

Watt, D. C., "The Security of Offshore Resources," *RUSI Journal for Defence Studies*, Vol. 123, June 1978, pp. 18-25.